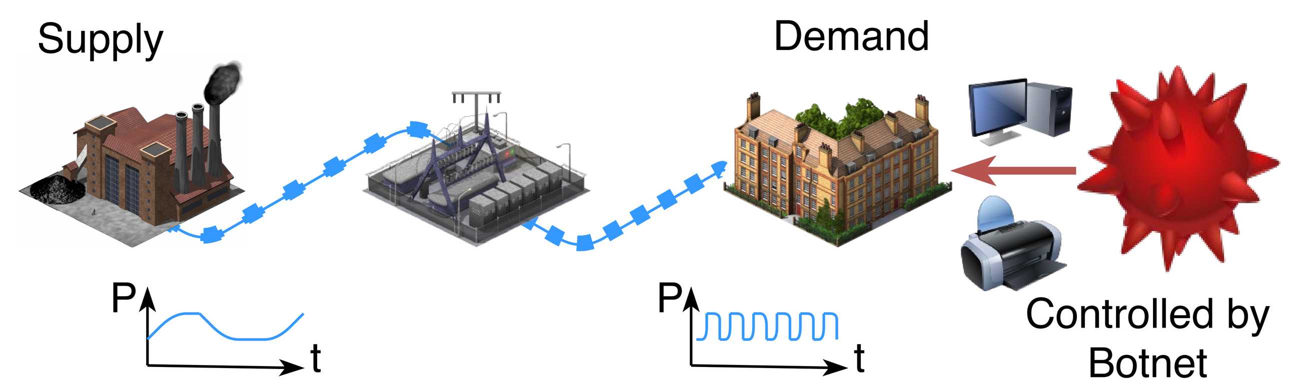
Grid Shock:

Coordinated Load-Changing Attacks on Power Grids

Adrian Dabrowski, Johanna Ullrich, Edgar Weippl

Competence Centers for Excellent Technologies
www.ffg.at/comet

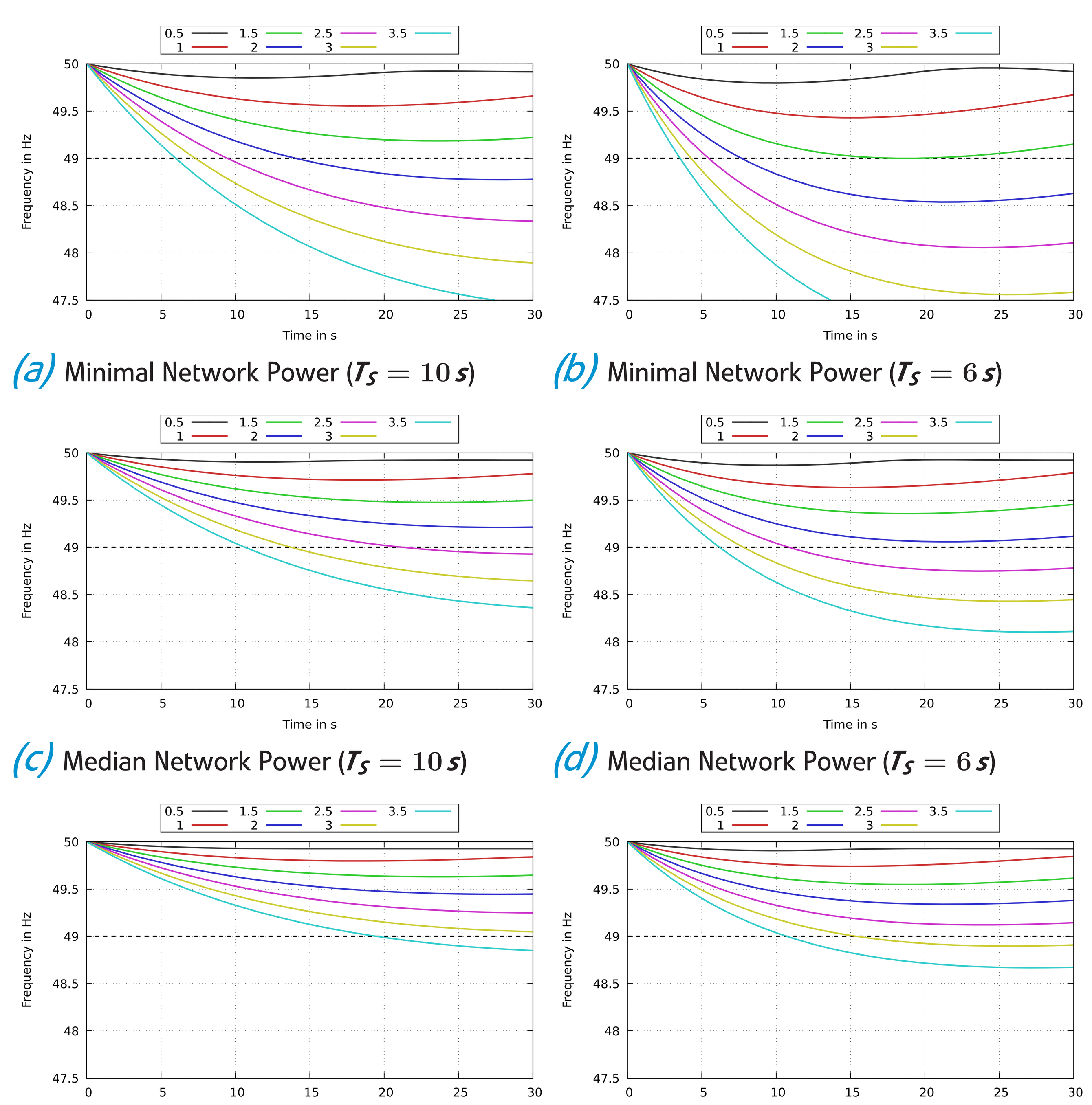
Problem & Motivation



Electric power grids are critical infrastructure. For reliable operation, providers have to continuously maintain a balance between supply and demand to keep the grid's nominal frequency of 50 Hz. In our work, we assume an adversary aiming to destabilize the power grid. Therefore, she builds a botnet of zombie computers and modulates their power consumption in a concerted fashion.

Static Load Attacks

In static load attacks, the adversary synchronously increases the electric load of the bots. The impact on the frequency is shown for a grid with high rotational inertia ($T_S = 10\,s$), i.e., predominantly fed by conventional power plants, and low rotational inertia ($T_S = 6\,s$), i.e., fed by a high share of renewables, at different levels of total network power. Static load attacks are in multiples of the ENTSO-E reference incident (3,000 MW).



(a) Minimal Network Power ($T_S = 10\,s$) *(b)* Minimal Network Power ($T_S = 6\,s$)
(c) Median Network Power ($T_S = 10\,s$) *(d)* Median Network Power ($T_S = 6\,s$)
(e) Maximum Network Power ($T_S = 10\,s$) *(f)* Maximum Network Power ($T_S = 6\,s$)

Figure 1: Impact of Static Load Attacks on Grid Frequency

Controllable Load

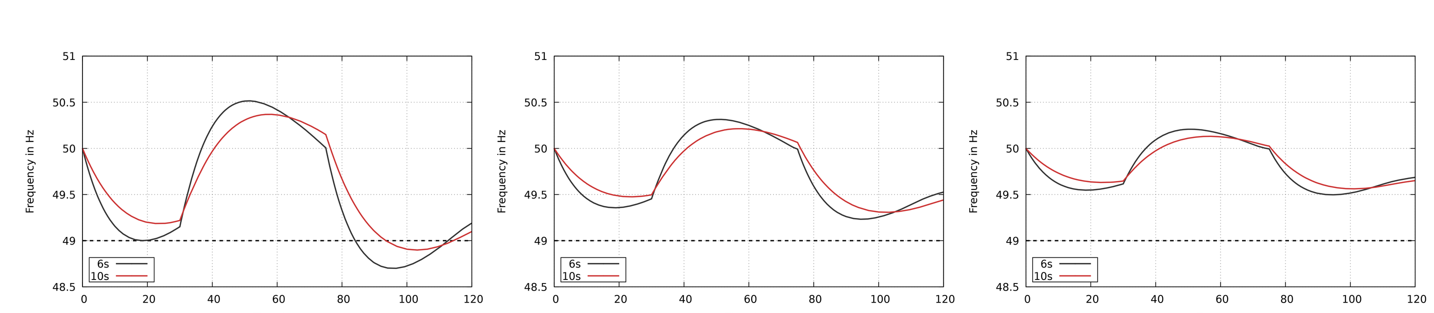
From our own measurements and data sheets, we compiled a table of controllable load by PC components and Internet-of-Things devices encompassing the potential for increasing and/or decreasing power, latencies of power modulation, and the amount of controllable load.

		Pwr Control		Latency		
Device	Type	Inc.	Dec.	on	off	Δ Load
CPU	Core2 Duo	●	○	20-60 ms	20-60 ms	35 W
	i3	●	○	20-60 ms	20-60 ms	55-73 W
	i5	●	○	20-60 ms	20-60 ms	73-95 W
	i7	●	○	20-60 ms	20-60 ms	77-95 W
	i7-E	●	○	20-60 ms	20-60 ms	130-150 W
GPU	Low-end	●	○	20-60 ms	20-60 ms	20-76 W
	Mid-end	●	○	20-60 ms	20-60 ms	102-151 W
	High-end	●	○	20-60 ms	20-60 ms	150-238 W
	Top-end	●	○	20-60 ms	20-60 ms	201-297 W
HDD		●	○	20-60 ms	20-60 ms	3-7 W
Screen TFT	size dep.	●	●	1-5 s	5-10 s	60-100 W
Laser Printer	SOHO	●	○	1-3 s	5-10 s	800-1300 W
Smart Air Cond.		●	○	1-10 s		600-1000 W
Smart Thermostat	elec. Heating	●	○	1-10 s		1-15 kW
Smart Oven		●	○	1-10 s		2-3 kW
Smart Refrigerator		●	○	1-10 s		300-500 W
Smart Kettle		●	○	1-10 s		1000-1500 W

Table 1: Latency and Achievable Load Differences

Dynamic Load Attacks

In dynamic load attacks, the adversary increases the load to the maximum and waits for the primary control to be activated; then, she decreases the load deactivating primary control again.



(a) Minimal Network Power *(b)* Median Network Power *(c)* Maximum Network Power

Figure 2: Impact of Dynamic Load Attacks on Grid Frequency

Conclusion

An adversary does not have to rely on smart grid features to modulate power consumption, given that an adequate communication infrastructure for striking the (legacy) power grid is currently nearly omnipresent: the Internet, to whom more and more power-consuming devices are connected. **Our simulations estimate that between 2.5 and 9.8 million infections are sufficient to attack the European synchronous grid.**

A. Dabrowski, J. Ullrich, E. Weippl, 2017, *Grid Shock: Coordinated Load-Changing Attacks on Power Grids*, Annual Computer Security Applications Conference (ACSAC).

SBA Research (SBA-K1) is a COMET Centre within the framework of COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG.